




**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

December 16, 2013

TO: Jonathan E. Fielding M.D., M.P.H., Director
Department of Public Health

FROM: Wendy L. Watanabe 
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – NURSE – FAMILY
PARTNERSHIP PROGRAM, TORRANCE OFFICE**

We have completed a review of the Department of Public Health's (DPH) Nurse-Family Partnership Program, Torrance Office's (NFP) compliance with the Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic Clinical Health (HITECH) Act.¹ On October 22, 2013, we provided your Department with our final draft report, and conducted an exit conference on November 21, 2013. This report includes our recommendations and your Department's response(s).

Approach/Scope

The purpose of the review was to evaluate NFP's compliance with HIPAA and the HITECH regulations, including best practices and relevant County and Departmental policies and procedures. The scope of this review included the *HIPAA Privacy Rule and HITECH Act Audit Tool*, which is a general assessment to determine whether the NFP is compliant with privacy, security, training, policies and procedures, and breach notification requirements. We noted that DPH follows the Department of Health Services' (DHS) HIPAA policies and procedures until they implement their own.

Our review covered the Privacy Rule requirements for: 1) notice of privacy practices for protected health information (PHI), 2) safeguards for PHI, 3) training, 4) complaint process, 5) refraining from intimidating or retaliatory acts, 6) uses and disclosures requiring authorization, 7) accounting for disclosures of PHI, 8) minimum necessary rule, and 9) HITECH Act Breach Notification Rule.

¹ 45 Code of Federal Regulations (CFR) Parts 160 and 164

Results of Review and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the Notice of Privacy Practices (NPP) to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.²

NFP management stated their public health nurses (PHNs) provide home visits to high-risk, low income pregnant youth until their first-born child is twenty-four months old. At the time of the review, the PHNs were not handing out the NPP and collecting the patient's written acknowledgment of receipt of the notice, and our review of patients' medical charts confirmed this. In addition, while NFP does not typically provide health care directly to patients in their office, we noted that the NPP was posted prominently at the time of our review.

During our facility walk-through, we found that the posted NPP did not include current contact information for U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), the County's Chief HIPAA Privacy Officer (CHPO), and DPH Privacy Officer, as required.

NFP is in partial compliance with the NPP standards.

Recommendations

- 1. Nurse-Family Partnership Program management must promptly instruct their Public Health Nurses to hand out the Notice of Privacy Practices to existing patients whose cases are currently open, and every new patient on the date of first service delivery. In addition, for those patients who are provided with the Notice of Privacy Practices, Public Health Nurses must make a good faith effort to obtain the patient's, or their representative's written acknowledgment of receipt of the notice.**
- 2. Department of Public Health and Nurse-Family Partnership Program management must promptly update the Notice of Privacy Practices with current contact information for the three agencies listed above.**

DPH's response indicates that they implemented our recommendations and are compliant with the Notices of Privacy Practices' posting standards.

² Ibid., § 164.520(c)

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information (PHI). A covered entity must reasonably safeguard PHI and electronic PHI, and prevent any disclosures that violate the Privacy Rule.

NFP management stated that medical charts are kept in the lockable cabinets near workforce members' work area; and, the cabinets are unlocked during business hours and locked at the end of the day by an assigned employee. Subsequent to this statement, we toured the facility and noted that the cabinets, while unlocked, were placed in an isolated area that is accessible to only workforce members who have a business need. Also, we noted the security guard, who sits by the entrance to NFP, provides added safeguards to protect the privacy of PHI, as patients or visitors are not allowed entry into NFP unless escorted by a workforce member or the security guard.

NFP management also reported that their computers are protected by endpoint protection software, which blocks downloading of PHI or other data to portable storage devices. In addition, NFP computers are configured to prevent workforce members from saving PHI onto their hard drives.

We verified that the fax machine, copier, and network printer were maintained in a secure area, and no PHI was left unattended during our review. To the extent that we were able to review NFP's administrative, technical, and physical safeguards, the facility appears to be in compliance with these standards.

Training

NFP, as a HIPAA covered program, must train all members of its workforce on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, to the extent necessary and appropriate for them to do their jobs. Workforce members include employees, volunteers, and trainees.

The DPH Office of Organizational Development and Training is responsible for ensuring its workforce members are trained on HIPAA compliance via the Learning Net. NFP management trains workforce members on DPH's HIPAA policies and procedures and additional, role-based training for their workforce members when applicable.

Our review of NFP training records showed that NFP is in 100% compliance with the training standards. All workforce members have completed the required HIPAA training. NFP management confirmed that they also trained workforce members on the DHS HIPAA policies, which are placed in a binder and accessible via the Department's intranet site. NFP is in compliance with the training standards.

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

NFP management informed us that the patient complaints are handled in accordance with DHS Policy 361.11, *Complaints Related to the Privacy of Protected Health Information (PHI)*, and workforce members will direct patients to contact the NFP Privacy Coordinator to file a complaint.

In the past year, no HIPAA complaints were filed with the CHPO by NFP patients. It appears that NFP is in compliance with complaint standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with NFP management confirm they are aware of their obligation to comply with DHS Policy 361.13, *Non-Retaliation*. They also understand that OCR will investigate complaints against a covered entity that assert retaliatory actions. In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by NFP patients. It appears that NFP is in compliance with the non-retaliation standards.

Uses and Disclosures Requiring Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

NFP management reported that they do not generally release patients' PHI other than for treatment. All patients of NFP, upon entering the program, are required to sign a State form, *Consent to Participate in the Nurse-Family Partnership Program and Authorization for Use and Disclosure of Medical information (Client)*. We reviewed the form and determined that this form does not meet the required elements for a valid HIPAA authorization. While this form may be sufficient consent for services, it is not sufficient for a HIPAA authorization to release patients' PHI.

Recommendation

- 3. Nurse-Family Partnership Program management must follow Department of Health Services Policy 361.4, *Use and Disclosure of***

Protected Health Information Requiring Authorization and use the associated authorization form until the Department of Public Health finalizes its Health Insurance Portability and Accountability Act policies.

DPH's response indicates while they have not had the need to disclose any PHI other than for the use of treatment, they agreed with our recommendation.

Accounting for Disclosures of Protected Health Information

The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures' log must be maintained in each patient's medical chart.

NFP management reported that while they follow DHS Policy 361.21, *Accounting of Disclosures of Protected Health Information*, the facility does not make any disclosures. NFP management affirmed that they will track non-routine disclosures of PHI if any are made, and will maintain the logs in the patients' medical charts. We provided additional guidance regarding accounting of disclosures to NFP management following the review.

NFP appears to be complying with the Accounting for Disclosures of PHI standards.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose.

Discussions with NFP management indicate that workforce members are aware of the minimum necessary standards. It appears that NFP is in compliance with the Minimum Necessary Rule standards.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered

entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

NFP management informed us that while they have not experienced a breach in their program, the workforce members are aware that they must report all incidents involving suspected or actual breaches to their immediate supervisors, who will report to DPH Privacy Officer. We noted from our review that DPH has a draft policy, *Responding to Breach or Suspected Breach of Protected Health Information*, and that it provides clear guidelines to workforce members in the event a breach or suspected breach of PHI is discovered. However, as of the date of this report, the final policy had not been issued to staff.

Recommendation

4. Department of Public Health management finalize its breach notification policy, and train workforce members on it.

DPH's response indicates that they are in the process of finalizing their breach notification policy for implementation.

Conclusion

Overall, our review indicates that NFP management is aware of and complying with HIPAA Privacy regulations. However, DPH's Office of Administrative Deputy needs to work with NFP to address the deficiencies noted in our review, and report any corrective action taken or pending to the HIPAA Compliance Office within 120 days from the receipt of this memorandum. We also wish to thank DPH's Privacy Officer and NFP managers and staff for their cooperation and assistance during this review.

Please call me if you have any questions, or your staff may contact Julia Chen, Assistant HIPAA Privacy Officer, at (213) 974-8315.

WLW:RGC:GZ:LTM:JC

Attachment

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
David Dykstra, Administrative Deputy, Department of Public Health
Judy Tan, Department of Public Health
Audit Committee
Health Deputies



COUNTY OF LOS ANGELES

Public Health

JONATHAN E. FIELDING, M.D., M.P.H.
Director and Health Officer

CYNTHIA A. HARDING, M.P.H.
Acting Chief Deputy Director

Maternal, Child, and Adolescent Health Programs

Suzanne M. Bostwick, Interim Director
600 South Commonwealth Avenue, Suite 800
Los Angeles, California 90005
TEL (213) 639-6400 • FAX (213) 427-6160
www.publichealth.lacounty.gov



BOARD OF SUPERVISORS

Gloria Molina
First District
Mark Ridley-Thomas
Second District
Zev Yaroslavsky
Third District
Don Knabe
Fourth District
Michael D. Antonovich
Fifth District

November 22, 2013

TO: Wendy L. Watanabe
Auditor-Controller

FROM: Suzanne Bostwick  for Suzanne Bostwick
Maternal, Child, & Adolescent Health Programs, Interim Director

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – NURSE – FAMILY
PARTNERSHIP PROGRAM, TORRANCE OFFICE**

This is our response to the Auditor-Controller's report on the Department of Public Health, Nurse-Family Partnership Program's (Torrance Office) compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Recommendations

1. Nurse-Family Partnership Program management must promptly instruct their Public Health Nurses to hand out the Notice of Privacy Practices to existing patients whose cases are currently open, and every new patient on the date of first service delivery. In addition, for those patients who are provided with the Notice of Privacy Practices, Public Health Nurses must make a good faith effort to obtain the patient's, or their representative's written acknowledgment of receipt of the notice.

Response:

Nurse Family Partnership appreciates the opportunity to be HIPAA reviewed in order to further strengthen our compliance to better protect the privacy of our clients.

Regarding recommendation #1, NFP management **agrees**.

Since the audit, further instructions have been given to the nurses regarding providing Notice of Privacy Practices (NPP) to the clients uniformly and placing a copy of the NPP and Acknowledgement of Receipt in the clients' charts. In addition, massive order of 3000 and more copies the NPP, both in English and Spanish, along with the Acknowledgement of Receipt have been placed and received to be distributed to the clients. As we speak, nurses are distributing, re-explaining NPP and obtaining clients' signatures of receipt.

- 2. Department of Public Health and Nurse-Family Partnership Program management must promptly update the Notice of Privacy Practices with current contact information for the three agencies listed above.**

Response: We agree.

The contact information on the NPP has been updated and NPP printed, received and in the process of distributing. The NPP posting on cubicle walls in the hall way has also been updated according to the DPH Website.

- 3. Nurse-Family Partnership Program management must follow Department of Health Services Policy 361.4, *Use and Disclosure of Protected Health Information Requiring Authorization* and use the associated authorization form until the Department of Public Health finalizes its Health Insurance Portability and Accountability Act policies.**

Response: We agree.

Thus far, NFP has not had the need to disclose any PHI other than for the use of treatment. We have recently received the authorization form from the DPH HIPAA Officer and will make it available to all staff and reiterate the use of the authorization form when appropriate.

Recommendation

- 4. Department of Public Health management finalize its breach notification policy, and train workforce members on it.**

Response: A copy of the draft breach notification policy no. 1237 was sent to County Counsel and the Chief HIPAA Privacy Office on October 15, 2013, for their review and approval, prior to implementation. The Department of Public Health also conducts HIPAA Awareness Training for all new workforce members that include breach notification and all current workforce members are also required to complete the HIPAA Update Training.

Wendy L. Watanabe
November 22, 2013
Page 3

Cc: Jonathan E. Fielding, Director and Health Officer of the Department of Public Health
David Dykstra, Administrative Deputy, Department of Public Health
Linda McBride, County HIPAA Privacy Office
Judy Tan, Compliance Officer, Department of Public Health
Julia Chen, County HIPAA Privacy Office
Jeanne Smart, Director, Nurse Family Partnership
Cindy Chow, Nurse Manager, Nurse Family Partnership
Todd McNairy, Chief of Staff, Maternal, Child, & Adolescent Health Programs
Yvonne Williams, NFP Public Health Nurse Supervisor